



FortiManager v5.0.9 Upgrade Guide



FortiManager v5.0.9 Upgrade Guide

October 23, 2014

02-509-257578-20141023

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log	4
FortiManager Firmware	5
Best practices	5
Firmware image naming convention.....	6
FortiManager VM firmware	6
SNMP MIB download	6
Build numbers.....	7
Firmware upgrade and support information	7
Upgrade Information	11
Upgrading from FortiManager v5.0.6, v5.0.7, or v5.0.8.....	11
Upgrading from FortiManager v5.0.5 or earlier	11
Firmware upgrade steps	12
Upgrading the FortiManager firmware for an operating cluster	14
Downgrading to previous firmware versions	14

Change Log

Date	Change Description
2014-10-23	Initial release.

FortiManager Firmware

This document provides an overview of FortiManager firmware and highlights general information you should be aware of prior to upgrading your FortiManager device. This guide is intended to supplement the [FortiManager Release Notes](#) documentation.

The following topics are included in this section:

- [Best practices](#)
- [Firmware image naming convention](#)
- [FortiManager VM firmware](#)
- [SNMP MIB download](#)
- [Build numbers](#)
- [Firmware upgrade and support information](#)

Best practices

Before any firmware upgrade complete the following:

- Download the FortiManager firmware image and Release Notes document from the [Fortinet Customer Service & Support](#) portal. Review the Release Notes including special notices, upgrade information, product integration and support, resolved and known issues.
- Prepare your FortiManager for upgrade. Install any pending configurations, ensure your managed devices are running the appropriate firmware versions as documented in the firmware Release Notes.
- Backup your configuration file. It is recommended that you create a system backup file and save this configuration to your local computer. The device configuration file is saved with a `.dat` extension.



In VM environments, it is recommended that you clone the VM instance. In the event of an issue with the firmware upgrade, you can revert to the VM clone.



In VM environments, upgrade your VM server to latest stable update and patch release offered by the VM host server provider.

-
- Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or managed devices.

- Once the upgrade is complete, test your FortiManager device to ensure that the upgrade was successful and that all managed devices are listed.



Firmware best practice: Stay current on patch releases for your current major release. Only upgrade to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the [FortiManager Release Notes](#) or contact Fortinet Technical Support.

Firmware image naming convention

FortiManager firmware images on the [Fortinet Customer Service & Support](#) portal HTTPS and FTP Download tabs are organized by firmware version, major release, and patch release. The firmware images in the folders follow a specific naming convention and each firmware image is specific to the device model. For example, the FMG_300D-v500-build0321-FORTINET.out image found in the */FortiManager/v5.00/5.0/5.0.7/* file folder is specific to the FortiManager 300D device model.

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for both VMware ESX/ESXi and Microsoft Hyper-V Server virtualization environments.

Microsoft Hyper-V Server

- FMG_VM64_HV-v500-buildxxxx-FORTINET.out: Download the firmware image to upgrade your existing FortiManager VM installation.
- FMG_VM64_HV-v500-buildxxxx-FORTINET.out.hyperv.zip: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

VMware ESX/ESXi

- FMG_VMxx-v500-buildxxxx-FORTINET.out: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiManager VM installations.
- FMG_VMxx-v500-buildxxxx-FORTINET.out.ovf.zip: Download either the 32-bit or 64-bit package for new FortiManager VM installations. The package contains a deployable Open Virtualization Format (OVF) virtual machine package for VMware ESX/ESXi installations and the fmg.vmdk and datadrive.vmdk virtual machine disk format files.

For more information see the FortiManager product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortimanager/virtualappliances.html>.

SNMP MIB download

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager v5.00 file folder.

Build numbers

FortiManager firmware images are generally documented as a three-digit build number. New FortiManager models may be released on a branch based off of the regular FortiManager firmware release. As such, the build number found in the *System Settings > General > Dashboard, System Information* widget and the output from the `get system status` CLI command displays this four-digit build number as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch point:` field that displays the regular three-digit build number.

Firmware upgrade and support information

The following table is for reference only. Review the applicable releases notes prior to upgrading your FortiManager system.



The following table uses the naming convention '4.3.7', where the first digit reflects the version, the second digit reflects the major release, and the third digit reflects the patch release. For example, 4.3.7 is v4.0 MR3 Patch Release 7.

Table 1: FortiManager upgrade and support information

FortiManager Firmware Version	Build Number	Upgrade From	FortiOS Version Support
v5.0			
5.0.9	0345	5.0.8 5.0.7	5.2.0, 5.2.1 5.0.4 to 5.0.9 4.3.2 and later 4.2.0 and later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.8	0342	5.0.7	5.2.0, 5.2.1 5.0.4 to 5.0.9 4.3.2 and later 4.2.0 and later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.7	0321	5.0.6	5.2.0, 5.2.1 5.0.4 to 5.0.9 4.3.2 and later 4.2.0 and later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-4000E, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			

Table 1: FortiManager upgrade and support information (continued)

FortiManager Firmware Version	Build Number	Upgrade From	FortiOS Version Support
5.0.6	0310	5.0.0 or later 4.3.0 or later	5.0.4 to 5.0.7 4.3.2 and later 4.2.0 and later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV. FMG-4000E is released on build 4046.			
5.0.5	0266	5.0.0 or later 4.3.0 or later	5.0.4 and 5.0.5 4.3.2 and later 4.2.0 and later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-1000D, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.4	0232	5.0.0 or later 4.3.0 or later	5.0.4 4.3.2 and later 4.2.0 and later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV.			
5.0.3	0200	5.0.0 or later 4.3.0 or later	5.0.3 4.3.2 and later 4.2.0 and later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-4000D, FMG-5001A, FMG-VM32, FMG-VM64, and FMG-VM64-HV. FMG-VM64-HV is released on build 0200. FMG-1000D is released on build 4035.			
5.0.2	0151	5.0.0 or 5.0.1 4.3.0 or later	5.0.2 4.3.2 and later 4.2.0 and later
Supported models: FMG-100C, FMG-200D, FMG-300D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64. FMG-300D is released on build 4020. FMG-4000D is released on build 4019.			
5.0.1	0121	5.0.0 4.3.0 or later	5.0.1 4.3.2 and later 4.2.0 and later
Supported models: FMG-100C, FMG-200D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64. FMG-300D is released on build 4009.			
5.0.0	0076	4.3.0 or later	5.0.0 4.3.2 and later 4.2.0 and later

Table 1: FortiManager upgrade and support information (continued)

FortiManager Firmware Version	Build Number	Upgrade From	FortiOS Version Support
Supported models: FMG-100C, FMG-200D, FMG-400B, FMG-400C, FMG-1000C, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
v4.3			
4.3.8	0719	4.3.1 or later 4.2.0 or later	4.3.5 and later 4.2.0 and later
Supported models: FMG-100, FMG-100C, FMG-200D, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.7	0700	4.3.1 or later 4.2.0 or later	4.3.5 and later 4.2.0 and later
Supported models: FMG-100, FMG-100C, FMG-200D, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.6	0673	4.3.1 or later 4.2.0 or later	4.3.2, 4.3.3, 4.3.4, 4.3.5, or 4.3.6 4.2.0 and later
Supported models: FMG-100, FMG-100C, FMG-200D, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.5	0658	4.3.1 or later 4.2.0 or later	4.3.2, 4.3.3, 4.3.4, or 4.3.5 4.2.0 and later
Supported models: FMG-100, FMG-100C, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64. Note: There is no image available for the FMG-200D.			
4.3.4	0640	4.3.1 or later 4.2.0 or later	4.3.2, 4.3.3, or 4.3.4 4.2.0 and later
Supported models: FMG-100, FMG-100C, FMG-200D, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.3	0631	4.3.1 or later 4.2.0 or later	4.3.2 or 4.3.3 4.2.0 and later
Supported models: FMG-100, FMG-100C, FMG-400A, FMG-400B, FMG-400C, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.2	0590	4.3.1 or later 4.2.0 or later	4.3.2 4.2.0 and later
Supported models: FMG-100, FMG-100C, FMG-400A, FMG-400B, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, FMG-VM32, and FMG-VM64.			
4.3.1	0524	4.3.0 4.2.0 or later	4.3.0 and 4.3.1 4.2.0 and later

Table 1: FortiManager upgrade and support information (continued)

FortiManager Firmware Version	Build Number	Upgrade From	FortiOS Version Support
Supported models: FMG-100, FMG-100C, FMG-400A, FMG-400B, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, FMG-5001A, and FMG-VM32. FMG-VM32 is released on build 6172.			
4.3.0	0514	4.2.1 or later	4.3.0 4.2.0 and later
Supported models: FMG-100, FMG-100C, FMG-400A, FMG-400B, FMG-1000C, FMG-3000, FMG-3000B, FMG-3000C, and FMG-5001A.			



In version 5.0, FortiClient endpoint agent configuration and management are now handled by the FortiGate Endpoint Control feature. You can configure your FortiGate device to discover new devices on your network, enforce FortiClient registration, and deploy a pre-configured endpoint profile to connected devices. This feature requires a FortiGate device running FortiOS v5.0.0 or later.

For more information, see the [Device and Client Reputation for FortiOS 5.0 Handbook](#) available in the [Fortinet Document Library](#).



FortiManager v5.0.0 introduced a new hard disk drive partition layout which is required for optimal usage and performance. Following an upgrade to FortiManager v5.0.0 or later, a backup must be made and then the disk must be reformatted with following command:

```
execute format {disk | disk-ext4}
```

A format will erase all local logs, and FortiGuard database information. Backup any local event logs that you wish to keep. The FortiManager will then need to re-download all of the AV/IPS/AS/WF objects from the FortiGuard Distribution Servers (FDS) which may take up to half a day. During that time managed devices will not be able to obtain these services from the FortiManager. You should configure devices to point to a backup FortiManager or the FDS for these services



When upgrading from FortiManager v4.0 MR2 EMS mode, you must run the *Import Wizard* for each managed device to ensure all rules and policies are added to the FortiManager.

Upgrade Information

This section outlines the general firmware upgrade steps. The following topics are included in this section:

- [Upgrading from FortiManager v5.0.6, v5.0.7, or v5.0.8](#)
- [Upgrading from FortiManager v5.0.5 or earlier](#)
- [Firmware upgrade steps](#)
- [Upgrading the FortiManager firmware for an operating cluster](#)
- [Downgrading to previous firmware versions](#)



Please review the [Firmware Release Notes](#) prior to upgrading.

Upgrading from FortiManager v5.0.6, v5.0.7, or v5.0.8

FortiManager v5.0.9 supports upgrade from v5.0.6, v5.0.7, or v5.0.8.

Upgrading from FortiManager v5.0.5 or earlier

FortiManager v5.0.7 or later has re-sized the flash partition storing system firmware. In order to accommodate the re-sizing, you **MUST** upgrade your device to v5.0.6 first. The secondary firmware and System Settings stored in the partition will be lost after upgrade. Please reconfigure System Settings as needed.

In VM environments, you will need to change the hard disk provisioned size to 513MB or more before powering on the FortiManager VM.



Upgrading your FMG-400B to v5.0.9 requires you to use an interim step. You **MUST** upgrade to v5.0.7 before upgrading to v5.0.9. For more information see the [FortiManager v5.0.7 Release Notes](#). The upgrade path looks like this:

v5.0.6 or earlier > v5.0.7 > v5.0.9



Please upgrade your FMG-5001A via the Web-based Manager or command line interface. Upgrade via TFTP from BIOS is not supported for this model.

Firmware upgrade steps

The following table lists the firmware upgrade steps.

Table 2: Upgrade steps

Step 1	Prepare your device for an upgrade.
Step 2	Backup your device configuration.
Step 3	For FortiManager VM, change the hard disk provisioned size to 513MB or more.
Step 4	Transfer the firmware image to your device.
Step 5	Log into the Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your device for an upgrade

1. Install any pending configurations.
2. Make sure all managed devices are running the supported firmware versions as stated in the [Firmware Release Notes](#).
3. Log in to the Fortinet Customer Service & Support portal at <https://support.fortinet.com>.
4. Select *Download* from the toolbar and select *Firmware Images* from the drop-down list.
5. Select *FortiManager* from the drop-down list and select the *HTTPS Download* tab.
Alternatively, you can select *FTP Download*. FTP is not an encrypted file transferring protocol and HTTPS download is recommended.
The image folders are displayed.
6. Browse to the appropriate file folder to download the firmware image (.out) and Release Notes document.
7. Select an image in the list to download the firmware image to your management computer.
8. To verify the integrity of the download, select *Download* from the toolbar and select *Firmware Image Checksums* from the drop-down list.
9. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

Step 2: Backup your device configuration

1. Go to *System Settings > Dashboard*.
2. Select *Backup* in the *System Information* widget.
The *Backup* dialog box opens.
3. Select the checkbox to encrypt the backup file and enter a password.



When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to your device.

4. Select **OK** and save the backup file on your local computer.



Optionally, you can backup the configuration file to a FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <ip> <path/filename save to  
the server> <username on server> < password> <crptpasswd>  
execute backup all-settings scp <ip> <path/filename save to the  
server> <SSH certificate> <crptpasswd>
```

For more information, see the [FortiManager CLI Reference](#).

Step 3: Change the FortiManager VM hard disk provisioned size

1. For VM environments, change the hard disk provisioned size to 513MB or more before upgrading your FortiManager VM.

Step 4: Transfer the firmware image to your device

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*.
The *Firmware Upgrade* dialog box opens.
3. Select *Browse* to locate the firmware package (.out file) that you downloaded from the [Customer Service & Support](#) portal and select *Open*.
4. Select **OK**. Your FortiManager will upload the firmware image and you will receive a confirmation message noting that the upgrade was successful.



Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to server> <IP of  
server> <username on server> <password>
```

For more information, see the [FortiManager CLI Reference](#).

Step 5: Log into the Web-based Manager to verify the upgrade was successful.

1. Refresh the browser and log back into the device.
2. Launch the *Device Manager* module and make sure that all formerly added devices are still listed.
3. Select each ADOM and make sure that managed devices reflect the appropriate connectivity state. Optionally, go to *System Settings > All ADOMs*.
4. Launch other functional modules and make sure they work properly.

Upgrading the FortiManager firmware for an operating cluster

You can upgrade the FortiManager firmware of an operating FortiManager cluster in the same way as upgrading the firmware of a standalone FortiManager unit. During the firmware upgrade procedure, you connect to the primary unit Web-based Manager or CLI to upgrade the firmware.

Similar to upgrading the firmware of a standalone FortiManager unit, normal FortiManager operations are temporarily interrupted while the cluster firmware upgrades. As a result of this interruption, you should upgrade the firmware during a maintenance window.

To upgrade FortiManager HA cluster:

1. Log into the primary unit Web-based Manager using the `admin` administrator account.
2. Upgrade the primary unit firmware. The upgrade is synchronized between the primary device and backup devices.

Administrators may not be able to connect to the FortiManager Web-based Manager until the upgrade synchronization process is complete. During the upgrade, using SSH or telnet to connect to the CLI may also be slow, however use the console to connect to the CLI.

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous FortiManager firmware release via the Web-based Manager or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

